

# SYSTEM AND METHOD FOR DECENTRALIZED AUTHENTICATION OF SERVER

**Publication number:** JP2000311138 (A)

**Publication date:** 2000-11-07

**Inventor(s):** YAMAGUCHI TAKAHIRO

**Applicant(s):** NIPPON ELECTRIC CO

**Classification:**

- international: **G06F21/20; G06F13/00; G06F15/00; H04L9/32; G06F21/20; G06F13/00; G06F15/00; H04L9/32; (IPC1-7): G06F15/00; G06F13/00; H04L9/32**

- European:

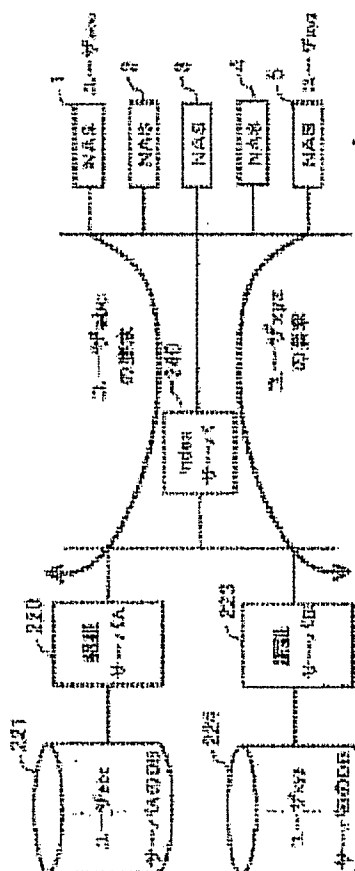
**Application number:** JP19990122966 19990428

**Priority number(s):** JP19990122966 19990428

## Abstract of JP 2000311138 (A)

**PROBLEM TO BE SOLVED:** To facilitate authentication even when the number of registered users increases by allowing an index server to retrieve the index of an authentication request and determine one of a plurality of authentication servers, and making the determined authentication server to authenticate the authentication request.

**SOLUTION:** The index server 240 is connected to a network and receives user authentication requests from network access servers 1, 2, 3, 4, and 5. Authentication servers 220 and 223 are connected to the index server 240 and the index server 240 determines an authentication server to perform authentication between the authentication servers 220 and 223. Then the authentication requests received from the network access servers 1, 2, 3, 4, and 5 are transferred to the determined authentication server. Consequently, the authentication can be facilitated even when the number of registered users increases.



Data supplied from the **esp@cenet** database — Worldwide

(19)日本国特許庁(JP)

(12) 公開特許公報(A)

(11)特許出願公開番号

特開2000-311138

(P2000-311138A)

(43)公開日 平成12年11月7日(2000.11.7)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	キーワード(参考)
G 0 6 F 15/00	3 3 0	C 0 6 F 15/00	3 3 0 A 5 B 0 8 6
13/00	3 5 1	13/00	3 6 1 Z 5 B 0 8 9
H 0 4 L 9/32		H 0 4 L 9/00	6 7 5 D 5 J 1 0 4

審査請求 有 請求項の数13 O L (全 10 頁)

(21)出願番号 特願平11-122966

(22)出願日 平成11年4月28日(1999.4.28)

(71)出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72)発明者 山口 恭弘

東京都港区芝五丁目7番1号 日本電気株式会社内

(74)代理人 100104400

弁理士 浅野 雄一郎

Fターム(参考) 5B085 AE23 BG07

5B089 GA11 JB22 KA05 KB06 KC44

KH03

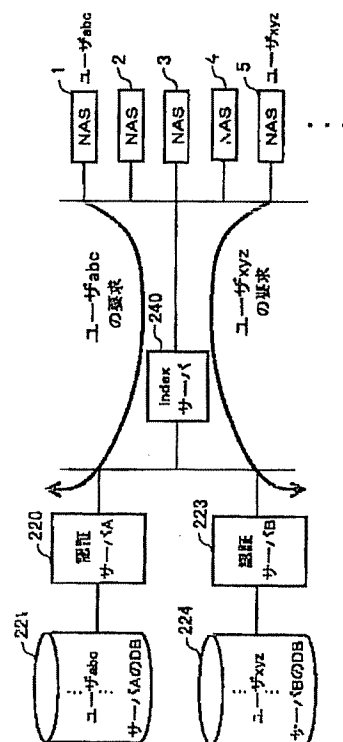
5J104 AA07 KA01 MA00 MA02 PA07

(54)【発明の名称】 サーバの分散認証システム及び方法

(57)【要約】

【課題】 登録ユーザ数の増加に対しても認証が容易にでき、データベースの増大を抑制でき、且つユーザ情報の変更に対して処理時間を短縮する。

【解決手段】 認証要求に対して認証を行うサーバの分散認証システムに、分散して認証を行う複数の認証サーバ220、221、223、224と、認証要求のインデックスを検索して複数の前記認証サーバから1つを決定し且つ決定した前記認証サーバに前記認証要求の認証を行わせるためのインデックスサーバ240とを備える。



# 【特許請求の範囲】

【請求項1】 認証要求に対して認証を行うサーバの分散認証システムにおいて、

分散して認証を行う複数の認証サーバと、

前記認証要求のインデックスを検索して複数の前記認証サーバから1つを決定し且つ決定した前記認証サーバに前記認証要求の認証を行わせるためのインデックスサーバとを備えることを特徴とするサーバの分散認証システム。

【請求項2】 複数の前記認証サーバの各々はデータベースを有し、前記データベースは、認証に用いる全ての認証データを前記認証サーバの分散数に応じて複数のグループに分割した分割認証データを有することを特徴とする、請求項1に記載のサーバの分散認証システム。

【請求項3】 複数の前記データベースに認証データを相互に重ねて持たせることにより、前記データベースの認証サーバに認証要求があった場合、前記インデックスサーバが連続して同一の認証サーバを決定するのを回避することを特徴とする、請求項2に記載のサーバの分散認証システム。

【請求項4】 さらに、データ管理サーバを設け、前記データ管理サーバは全ての前記認証データを管理し、前記認証データに変更があると、前記データベースの分割認証データを更新することを特徴とする、請求項2に記載のサーバの分散認証システム。

【請求項5】 前記データ管理サーバは、前記認証要求のインデックスと同一のインデックスが付された全ての前記認証データをソートし、ソートの順番に従って全ての前記認証データを複数のグループに分割して管理することを特徴とする、請求項2に記載のサーバの分散認証システム。

【請求項6】 前記インデックスサーバはインデックスファイルを有し、前記インデックスファイルは全てのインデックスを前記認証サーバの分散数に応じて複数のグループに分割して管理し、前記認証要求のインデックスがどこの前記グループに属するかを検索して認証サーバを決定するように管理することを可能にすることを特徴とする、請求項1に記載のサーバの分散認証システム。

【請求項7】 前記インデックスファイルは全てのインデックスをソートし、ソートの順番に従って前記全てのインデックスを複数のグループに分割し管理することを特徴とする、請求項6に記載のサーバの分散認証システム。

【請求項8】 さらに、データ管理サーバを設け、前記データ管理サーバは全ての前記インデックスを管理し、前記インデックスに変更があると、グループ毎に前記インデックスファイルを更新することを特徴とする、請求項6に記載のサーバの分散認証システム。

【請求項9】 前記認証サーバは認証結果を返却するとき、前記認証サーバのIPアドレスを前記インデックス

サーバのIPアドレスに変換して発信元のアドレスとすることを特徴とする、請求項1に記載のサーバの分散認証システム。

【請求項10】 前記インデックスサーバは、認証要求に対して検索の結果、複数の前記サーバから1つを決定できない場合、要求不適合の応答を行うことを特徴とする、請求項1に記載のサーバの分散認証システム。

【請求項11】 前記インデックスサーバは、認証要求に対して検索の結果、複数の前記認証サーバから1つを決定できない場合、特定の認証サーバに前記認証要求を転送して前記特定認証サーバから要求不適合の応答を行うようにすることを特徴とする、請求項1に記載のサーバの分散認証システム。

【請求項12】 認証要求に対して認証を行うサーバの分散認証システムにおいて、

分散して認証を行う複数の認証サーバと、

複数の前記認証サーバの認証に用いる全ての認証データを前記認証サーバの分散数に応じて複数のグループに分割した分割認証データを有する複数のデータベースと、前記認証要求のインデックスを検索して複数の前記認証サーバから1つを決定し且つ決定した前記認証サーバに前記認証要求の認証を行わせるためのインデックスサーバと、

全てのインデックスを前記認証サーバの分散数に応じて複数のグループに分割して保持し、且つ前記インデックスサーバにより前記認証要求のインデックスがどこの前記グループに属するかを検索し認証サーバを決定するためのインデックスファイルと、

全ての前記認証データを管理し前記認証データに変更があると、前記データベースの分割認証データを更新し、且つ前記インデックスファイルのインデックスを変更する前記データ管理サーバとを備えることを特徴とするサーバの分散認証システム。

【請求項13】 認証要求に対して認証を行うサーバの分散認証方法において、複数の認証サーバに分散して認証を行う工程と、

前記認証要求のインデックスを検索して複数の前記認証サーバから1つを決定し且つ決定した前記認証サーバにより前記認証要求の認証を行う工程とを備えることを特徴とするサーバの分散認証方法。

## 【発明の詳細な説明】

### 【0001】

【産業上の利用分野】本発明はサーバの認証システムに関する。特に、本発明は、極めて多数のユーザをかかえるネットワークで認証要求を短時間に処理するサーバの分散認証システム及び方法に関する。

### 【0002】

【従来の技術】従来、認証を行う認証サーバは、複数のアクセスポイントを持つネットワークに対し、ユーザがどのアクセスポイントからアクセスしてもユーザの正当

性を確認できるようにするために導入されたものである。そのため、1台の認証サーバでネットワークにおける全てのユーザの情報が管理されている。また、実用に耐え得るサーバの応答時間はせいぜい1〜2秒程度と非常に短い。

【0003】ネットワークに登録されるユーザが増加すると、この応答時間は2つの点で問題を抱えることになる。1つは巨大なユーザデータのデータベースから特定のユーザの認証データを検索するのに要する時間が大きくなる点であり、1つは複数のユーザからの認証要求を同時に受ける頻度が高くなり、認証サーバの負荷が増大する可能性があり認証するのに要する時間が大きくなる点である。

【0004】前者の点を避けるために高速コンピュータを導入する必要がある。しかし、この導入により検索の時間が短縮できるが、登録ユーザの著しい増加に対しては、この導入にも限界があるという問題がある。また、後者の点を避けるために、複数の認証サーバを設置し、ネットワークアクセスサーバ(NAS)毎に登録が行われる認証サーバを振り分けて複数ユーザの同時要求の頻度を下げる方法が考えられる。この方法について以下に説明を行う。

【0005】図10は従来のサーバの認証システムを示す図である。本図に示すように、複数のネットワークアクセスサーバ(NAS)71は認証サーバA73に対してユーザの正当性を確認する認証要求を行い、また、複数のネットワークアクセスサーバ72は認証サーバB74に対して認証要求を行う。認証サーバA73は全認証データベース76を有し、認証サーバB74は全認証データベース77を有する。認証サーバA72、認証サーバB74のどちらにアクセスしても認証できるように、全認証データベース76、77の各々では全登録ユーザを検索対象として作成した同一のファイルが管理される。

【0006】全認証データベース76、77はデータベース管理サーバ75によって管理される。データベース管理サーバ75にはデータベースが設けられ、データベース管理サーバ75のデータベースはユーザ情報に関するファイルを管理する。そして、ユーザ情報の変更に伴ってデータベース管理サーバ75におけるデータベース上のファイルが更新される。

【0007】データベース管理サーバ75のデータベースと、認証ベースA73の全認証データベース76及び認証ベースB74の全認証データベース77との内容を一致させる必要がある。この場合、認証ベースA73の全認証データベース76及び認証ベースB74の全認証データベース77はデータベース管理サーバ75のデータベースから更新されたファイルを転送して貰い更新される。

【0008】このように、ユーザのアクセスは認証サーバ

A73と、認証サーバ74に分散されるので、同時要求の頻度を低下して認証の時間を短縮できる。しかしながら、上記サーバの認証システムでは、同一の全認証データベース76、77が重ねて設置される。さらに、登録ユーザ数が著しく増加するにつれて、設置数の増加と共にデータベース当たりのファイルサイズも飛躍的に増大し、コストが増大するという問題がある。

【0009】また、ユーザ情報の変更に伴って、複数の全認証データベース76、77が更新されなければならない。このため、逆に、更新の処理に要する時間が大きくなるという問題がある。認証要求があったときに、更新処理を行っている、と、応答時間が長くなるためである。

【0010】

【発明が解決しようとする課題】したがって、本発明は上記問題点を鑑みて、登録ユーザ数の増加に対しても認証が容易にでき、データベースの増大を抑制でき、且つユーザ情報の変更に対して処理時間を短縮できるサーバの分散認証システム及び方法を提供することを目的とする。

【0011】

【課題を解決するための手段】本発明は前記問題点を解決するために、認証要求に対して認証を行うサーバの分散認証システムにおいて、分散して認証を行う複数の認証サーバと、前記認証要求のインデックスを検索して複数の前記認証サーバから1つを決定し且つ決定した前記認証サーバに前記認証要求の認証を行わせるためのインデックスサーバとを備えることを特徴とするサーバの分散認証システムを提供する。この手段により、インデックスサーバの導入により認証要求の分散が実現でき、分散した認証サーバで認証が行われるので登録ユーザ数の増加に対して認証が容易になった。認証を容易にするための改造は小規模であり、ユーザ情報の変更に対してファイル転送を少なくできる。

【0012】好ましくは、複数の前記認証サーバの各々はデータベースを有し、前記データベースは、認証に用いる全ての認証データを前記認証サーバの分散数に応じて複数のグループに分割した分割認証データを有する。この手段により、データベースのファイル数は認証サーバに必要なサイズになるので、登録ユーザ数の増加に対してデータベースの増大を抑制することが可能になった。

【0013】好ましくは、複数の前記データベースに認証データを相互に重ねて持たせることにより、前記データベースの認証サーバに認証要求があった場合、前記インデックスサーバが連続して同一の認証サーバを決定するのを回避する。この手段により、同一の認証サーバの決定が回避され同時認証も回避されるので、登録ユーザ数の増加に対して認証サーバの負荷を軽減できる。好ましくは、さらに、データ管理サーバを設け、前記データ

管理サーバは全ての前記認証データを管理し、前記認証データに変更があると、前記データベースの分割認証データを更新し、前記認証要求のインデックスと同一のインデックスが付された全ての前記認証データをソートし、ソートの順番に従って全ての前記認証データを複数のグループに分割する。この手段により、データベース毎に整理されたファイルで更新が行われるので、ユーザ情報の変更に対して更新ファイルの転送時間を軽減できる。

【0014】好ましくは、前記インデックスサーバはインデックスファイルを有し、前記インデックスファイルは全てのインデックスを前記認証サーバの分散数に応じて複数のグループに分割され、前記認証要求のインデックスがどこの前記グループに属するかを検索して認証サーバが決定され、全てのインデックスをソートし、ソートの順番に従って前記全てのインデックスを複数のグループに分割する。このように、インデックスサーバには単純な処理を行わせて負荷を軽くして、全ての認証要求を受け付けさせる。

【0015】好ましくは、さらに、データ管理サーバを設け、前記データ管理サーバは全ての前記インデックスを管理し、前記インデックスに変更があると、グループ毎に前記インデックスファイルを更新する。この手段により、インデックスファイルがグループ毎に更新されるので、更新にかかる時間を短縮できる。

【0016】好ましくは、前記認証サーバは認証結果を返却するとき、前記認証サーバのIPアドレスを前記インデックスサーバのIPアドレスに変換して発信元のアドレスとする。この手段により、全ての応答が、分散した認証サーバからではなく、インデックスサーバから返却されるようにみせることができる。このため、ユーザに違和感を与えないようにできる。

【0017】好ましくは、前記インデックスサーバは、認証要求に対して検索の結果、複数の前記サーバから1つを決定できない場合、要求不適合の応答を行う。この手段により、インデックスサーバで転送先の無い認証要求が処理される。好ましくは、前記インデックスサーバは、認証要求に対して検索の結果、複数の前記認証サーバから1つを決定できない場合、特定の認証サーバに前記認証要求を転送して前記特定認証サーバから要求不適合の応答を行うようにする。この手段により、特定の認証サーバで、転送先の無い認証要求が処理される。

【0018】さらに、本発明は認証要求に対して認証を行うサーバの分散認証システムにおいて、分散して認証を行う複数の認証サーバと、複数の前記認証サーバの認証に用いる全ての認証データを前記認証サーバの分散数に応じて複数のグループに分割した分割認証データを有する複数のデータベースと、前記認証要求のインデックスを検索して複数の前記認証サーバから1つを決定し且つ決定した前記認証サーバに前記認証要求の認証を行わ

せるためのインデックスサーバと、全てのインデックスを前記認証サーバの分散数に応じて複数のグループに分割して保持し、且つ前記インデックスサーバにより前記認証要求のインデックスがどこの前記グループに属するかを検索し認証サーバを決定するためのインデックスファイルと、全ての前記認証データを管理し前記認証データに変更があると、前記データベースの分割認証データを更新し、且つ前記インデックスファイルのインデックスを変更する前記データ管理サーバとを備えることを特徴とするサーバの分散認証システムを提供する。

【0019】この手段により、上記発明と同様に、認証に対して素早い応答が可能になり、応答を早くするための改造は小規模であり、ユーザ情報の変更に対してファイル転送を少なくできる。

【0020】さらに、本発明は、認証要求に対して認証を行うサーバの分散認証方法において、複数の認証サーバに分散して認証を行う工程と、前記認証要求のインデックスを検索して複数の前記認証サーバから1つを決定し且つ決定した前記認証サーバにより前記認証要求の認証を行う工程とを備えることを特徴とするサーバの分散認証方法を提供する。この手段により、上記発明と同様に、認証に対して素早い応答が可能になり、応答を早くするための改造は小規模であり、ユーザ情報の変更に対してファイル転送を少なくできる。

【0021】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照して説明する。図1は本発明に係るサーバの分散認証システムの概略構成例を示すブロック図である。本図に示すように、サーバの分散認証システムにおいて、ネットワークに複数のネットワークアクセスサーバ(NAS)1、2、3、4、5が接続され、ネットワークアクセスサーバ1、2、3、4、5の各々はユーザからのアクセス要求を受け、ユーザの認証の可否を問うために認証要求を送出する。ネットワークにはインデックス(Index)サーバ240が接続され、インデックスサーバ240は複数のネットワークアクセスサーバ1、2、3、4、5からユーザの認証要求を受け取る。

【0022】インデックスサーバ240には分散された認証サーバA220、認証サーバB223が接続され、インデックスサーバ240は、分散された認証サーバA220、認証サーバB223のうち認証を行わせる認証サーバを決定し、決定した認証サーバにネットワークアクセスサーバ1、2、3、4、5から受け取った認証要求を転送する。このように、インデックスサーバ240は、ユーザがどの認証サーバにおいて認証されるべきかを判断して、適切な認証サーバに認証要求を転送するために設けられる。

【0023】また、分散された認証サーバA220、認証サーバB223の各々には認証サーバのデータベース(DB)221、認証サーバのデータベース(DB)2

24がそれぞれ設けられる。認証サーバA220のデータベース(DB)221、認証サーバB223のデータベース(DB)224の各々には全登録ユーザが2つに分けられた1つのグループに関する登録ユーザの認証情報のファイルが管理されている。

【0024】一例として、データベース221にはユーザabcの認証情報を含むファイルが管理され、データベース223にはユーザxyzの認証情報を含むファイルが管理されているとする。ユーザabcからネットワークアクセスサーバ1にアクセス要求があると、インデックスサーバ240は認証サーバA220に認証要求を転送する。ユーザxyzからネットワークアクセスサーバ5にアクセス要求があると、インデックスサーバ240は認証サーバB223に認証要求を転送する。

【0025】このようにして、認証要求は、インデックスサーバ240によって受け取られ、分散された認証サーバA220、認証サーバB223のうち適切な方に転送されるので、認証サーバA220、認証サーバB223の各々は同時に認証要求を受ける頻度が低下し応答時間が短縮することになる。また、ユーザの認証情報のファイルはデータベース221、224に分けて管理されるので、登録ユーザ数の増加に応じてデータファイルのサイズが増大するのを抑制することができるようになった。

【0026】また、ユーザの認証情報のファイルに関する更新も、データベース221、224のうちユーザ情報の変更が生じた方について行えばよいので、更新処理のためのファイル転送の時間を短くできるようになった。

【0027】図2は図1におけるサーバの分散認証システムの具体例を説明する図である。本図に示すように、サーバの分散認証システムにはデータ管理サーバ210が設けられ、データ管理サーバ210はネットワークの全登録ユーザのデータを管理し、そのデータを各認証サーバ用の認証データベースに変換、作成し、且つ各登録ユーザの認証データがどの認証サーバにあるかを示すインデックスファイルを作成するデータベース作成機能部211と、作成したデータベースを認証サーバに転送する機能部212と、インデックスファイルを後述するインデックスサーバ240のインデックスファイル241に転送するインデックス転送機能部213とを具備する。

【0028】さらに、ネットワークに接続されるインデックスサーバ240はインデックスファイル241を保持し、且つネットワークアクセスサーバ25からの認証を受け付ける要求受付機能部242と、インデックスファイル241から認証要求の転送先を探すサーバ検索機能部243と、探した転送先に認証要求を送る要求転送機能部244とを具備する。

【0029】また、分散した認証サーバA220、認証

サーバB223は基本的にRADIUSプロトコルに従う通常のRADIUSサーバであり、認証結果を返却する場合に、応答パケットの自分のIP(Internet Protocol)アドレスをインデックスサーバ240のIPに書き換える機能部222、225をそれぞれ有する。なお、認証サーバA220、認証サーバB223は、前述したように、認証サーバAのデータベース(DB)221、認証サーバBのデータベース224を有する。

【0030】図3は図2のデータ管理サーバ210の例を説明する図である。データ管理サーバ210のデータベース作成機能部211においてデータベースを作成するときには、本図に示すように、全登録ユーザのデータ31はユーザ名をインデックスとして昇順に、例えば、インデックスaaa、aab、…、mzz、naa、…、zzzのように、ソートされ、2つの登録ユーザの認証データ32Aと32Bとに、例えば、インデックスのaaa、…、mzz認証データと、インデックスのnaa、…、zzz認証データとのように、ソートの順番に分割される。分割されたインデックスaaa～mzzの登録ユーザの認証データ32A、分割されたnaa～zzzのユーザの認証データ32Bは、データ管理サーバ210の認証データベース211A、認証データベース211Bでそれぞれ管理される。なお、登録ユーザの認証データ32A、32BはBSD UNIXのdbm形式のファイルに変換される。

【0031】図4は図2のインデックスファイル241の構成例を示す図である。本図に示すように、第1行は認証サーバA220の情報を表す。第1列41は認証サーバA220のデータベース221のソート順で先頭にくるユーザ名のインデックスを表す。第2列42はソート順で末尾にくるユーザ名のインデックスを表す。第3列43は認証サーバA220自体を表す。

【0032】第2行は認証サーバB223の情報を表す。第1列41は認証サーバB223のデータベース224のソート順で先頭にくるユーザ名のインデックスを表す。第2列42はソート順で末尾にくるユーザ名のインデックスを表す。第3列43は認証サーバB223の第1行が認証サーバA220の情報を表す。第1列41は認証サーバA220のデータベース221のソート順で先頭にくるユーザ名のインデックスを表す。第2列42はソート順で末尾にくるユーザ名のインデックスを表す。第3列43は認証サーバA220自体を表す。

【0033】なお、ユーザ情報の変更があると、データ管理サーバ210は認証サーバA220、認証サーバB223のデータベース221、224と、インデックスサーバ240のインデックスファイル241とを更新する。

【0034】図5はユーザの認証要求の処理例を説明するフローチャートである。本図に示すように；ステップ

S1において、ネットワークアクセスサーバ25からインデックスサーバ240宛てにユーザabcの認証要求(261)のパケットが送出される。ステップS2において、インデックスサーバ240の要求受付機能部242がネットワークアクセスサーバ25の認証要求(261)を受け付ける。

【0035】ステップS3において、サーバ検索機能部243は、受け付けられた認証要求に基づいて、インデックスファイル241に対して認証サーバの検索を行う。すなわち、サーバ検索機能部243では、送出してきたパケットがユーザabcの認証要求を求めるものであることを知り、ユーザabcのインデックスファイル241の第1行第1列(41;図4参照)aaaから第1行第2列(42)mzzの間にあることからユーザabcの認証情報が存在し得るのは認証サーバA220(43)であることを知る。

【0036】ステップS4において、要求転送機能部244は検索された認証サーバA220に認証要求(262)のパケットを転送する。ステップS5において、認証サーバA220はこの認証要求の認証を行い、認証結果をネットワークアクセスサーバ25に直接返却する。この際、認証サーバA220はアドレス変換機能部222を使って発信元のIPアドレスをインデックスサーバ240のIPアドレスに書き換える。認証結果の返却時にユーザに違和感を与えないためである。

【0037】図6はユーザの認証要求について別の処理例を説明するフローチャートである。本図に示すように;ステップS11において、ネットワークアクセスサーバ25からインデックスサーバ240宛てにユーザxyzの認証要求(271)のパケットが送出される。ステップS12において、インデックスサーバ240の要求受付機能部242がネットワークアクセスサーバ25の認証要求(271)を受け付ける。

【0038】ステップS13において、サーバ検索機能部243はインデックスファイル241に対して認証サーバの検索を行う。すなわち、サーバ検索機能部243では、送出してきたパケットがユーザxyzの認証要求を求めるものであることを知り、ユーザxyzのインデックスファイル241の第1行に合致せず、第2行第1列(41;図4参照)naaから第2行第2列(42)zzzの間にあることからユーザxyzの認証情報が存在し得るのは認証サーバB223(43)であることを知る。

【0039】ステップS14において、要求転送機能部244は検索された認証サーバB223に認証要求(272)のパケットを転送する。ステップS15において、認証サーバB223はこの認証要求の認証を行い、認証結果をネットワークアクセスサーバ25に直接返却する。この際、認証サーバB223はアドレス変換機能部225を使って発信元のIPアドレスをインデックス

サーバ240のIPアドレスに書き換える。前述と同様に、認証結果の返却時にユーザに違和感を与えないためである。

【0040】図7はユーザの認証要求について、さらに、別の処理例を説明するフローチャートである。本図に示すように;ステップS21において、ネットワークアクセスサーバ25からインデックスサーバ240宛てにユーザ123の認証要求(281)のパケットが送出される。ステップS21において、インデックスサーバ240の要求受付機能部242がネットワークアクセスサーバ25の認証要求(281)を受け付ける。

【0041】ステップS23において、サーバ検索機能部243によるインデックスファイル241により認証サーバの検索が行われる。ステップS24において、すなわち、サーバ検索機能部243では、送出してきたパケットがユーザ123の認証要求を求めるものであることを知り、ユーザ123のインデックスファイル241の第1行、第2行に合致せず、合致するものが無い場合には、分散した各認証サーバA221、認証サーバB223に認証要求を行うことが不適合(NG)であるとの検索結果を行う。

【0042】ステップS25において、この場合、サーバ検索機能部243では異常応答機能部245に認証要求(282)が転送される。ステップS26において、異常応答機能部245からネットワークアクセスサーバ25に不適合(NG)の結果(283)が返却される。なお、ネットワークアクセスサーバ25はいずれの場合もインデックスサーバ240に対して認証要求を送るが、実際にはその返答が返ってくる先は送った認証要求の中のユーザ名によって異なる。しかし、ネットワークアクセスサーバ25にとって全ての応答はインデックスサーバ240から返ってくるように見える。ユーザに違和感を与えないためである。

【0043】図8は図2のサーバの分散認証システムを拡張した例を示す図である。本図には、4台の分散した認証サーバA220、認証サーバB223、認証サーバC226、認証サーバC229が示されるが、その数はさらに拡張することができる。図9は図8のインデックスファイル241の構成例を示す図である。本図に示すように、インデックスファイル241は、図4と同じフォーマットで行数を増やす。

【0044】なお、認証データベースの一部あるいは全部を複数の認証サーバに持たせることができる。図9に示す例では、登録ユーザaaaから登録ユーザcccまでは認証サーバA220及び認証サーバB223の双方で認証を受けることができるようにする。この場合、インデックスサーバ240に転送先制御機能部245を追加して設け、転送先制御機能部245は複数の転送先候補があるとき、より最近転送していない方に転送させる。つまり、連続して同一の認証サーバに認証要求を転

送しないようにするためである。これにより同時認証要求に対してきめ細かい制御を行なうことが可能になる。例えば、ユーザmmmの認証要求は認証サーバB223に転送されるが、ユーザabcの認証要求は認証サーバA220でも認証サーバB223でも要求を受けることができる。しかし、認証サーバB223には前の要求を送ったばかりなので、ユーザabcの認証要求は、認証サーバA220に転送される。

【0045】また、転送先の無い要求をインデックスサーバ240自身に処理させずに、特定の認証サーバに転送させることもできる。このため、図9の最下行を第1列、第2列とも空欄にし、転送先を、例えば、認証サーバA220にし、これを転送先が無い場合と定義する。このようにして、この空欄は、認証サーバA220での異常ログインなどに役立てることができる。

【0046】

【発明の効果】以上説明したように、本発明によれば、第1の効果として、認証要求に対する素早い応答が期待できる。その理由は、認証サーバを複数設置することにより、認証の負荷を分散させることができるからである。また、登録ユーザ数の増大に対してデータベースの増大を抑制でき、データベースでの認証時間が短くなるからである。

【0047】第2の効果として、ファイル転送のコストを抑制することができる。その理由は、認証データベースを分割して、必要なサーバに分割ファイルのみを送ることができるからである。第3の効果として、従来の認証システムに対して認証の分散のために加える使用の改造量が小さくてすむことにある。

【0048】その理由は、インデックスサーバを認証サーバとみなして認証要求を送ることができ、ネットワークアクセスサーバ側からは複数の認証サーバを意識しなくてすむからである。上述のように、インデックスサーバは全ての認証要求を受け付けることになるが、インデックスファイルを判断して認証サーバを決めるだけなので、その負荷は高くないことにある。

【図面の簡単な説明】

【図1】本発明に係るサーバの分散認証システムの概略構成例を示すブロック図である。

【図2】図1におけるサーバの分散認証システムの具体

例を説明する図である。

【図3】図2のデータ管理サーバ210の例を説明する図である。

【図4】図2のインデックスファイル241の構成例を示す図である。

【図5】ユーザの認証要求の処理例を説明するフローチャートである。

【図6】ユーザの認証要求について別の処理例を説明するフローチャートである。

【図7】ユーザの認証要求について、さらに、別の処理例を説明するフローチャートである。

【図8】図2のサーバの分散認証システムを拡張した例を示す図である。

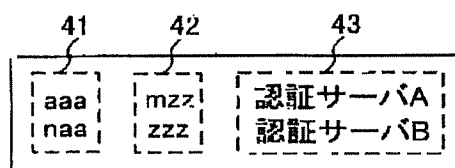
【図9】図8のインデックスファイル241の構成例を示す図である。

【図10】従来のサーバの認証システムを示す図である。

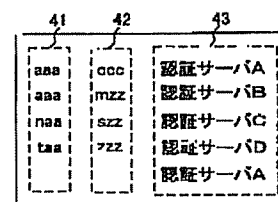
【符号の説明】

1～5、25…ネットワークアクセスサーバ  
210…データ管理サーバ  
211…データベース作成機能部  
211A、211B…認証DB  
212…データベース転送機能部  
213…インデックス転送機能部  
220…認証サーバA  
221…サーバAのDB  
222、225、228、231…アドレス変換機能部  
223…認証サーバB  
224…サーバBのDB  
226…認証サーバC  
227…サーバCのDB  
229…認証サーバD  
230…サーバDのDB  
240…インデックスサーバ  
241…インデックスファイル  
242…要求受付機能部  
243…サーバ検索機能部  
244…要求転送機能部  
245…異常応答機能部

【図4】

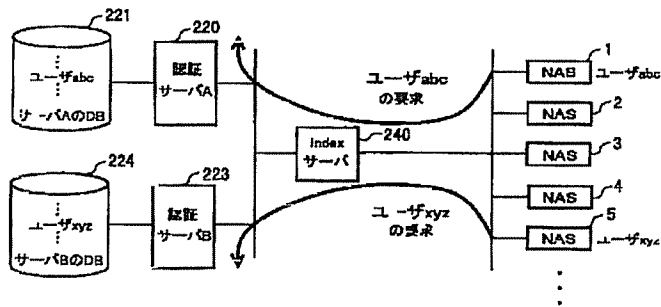


【図9】

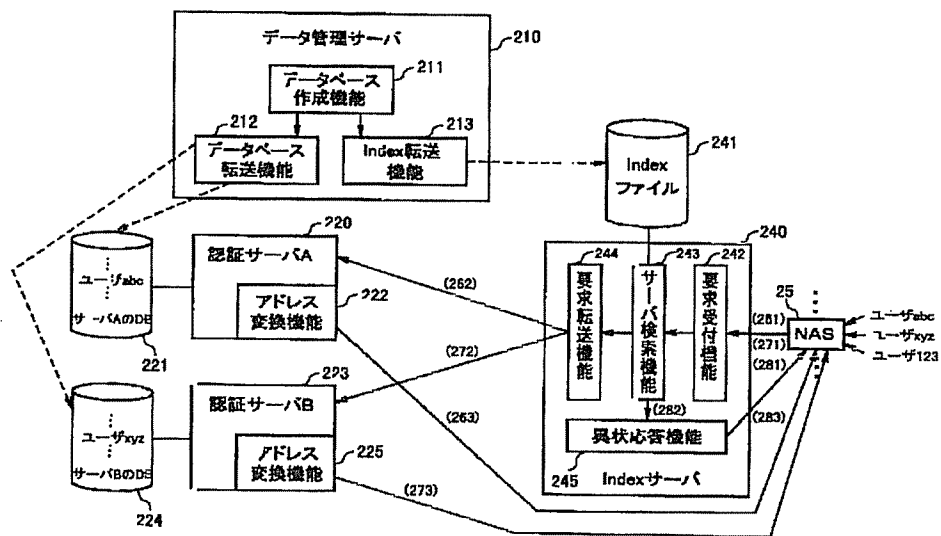




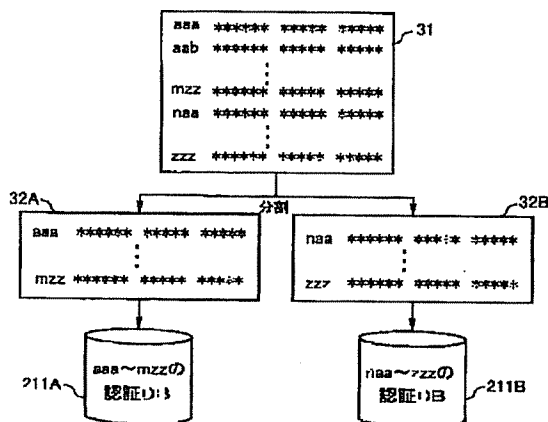
【図1】



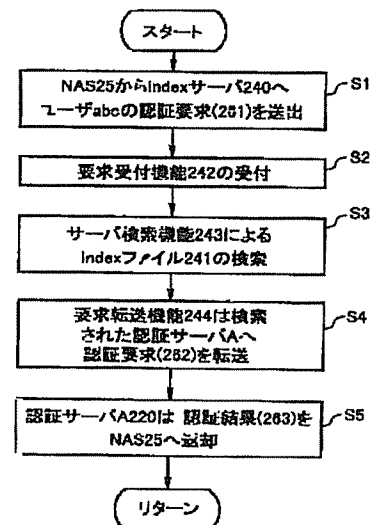
【図2】



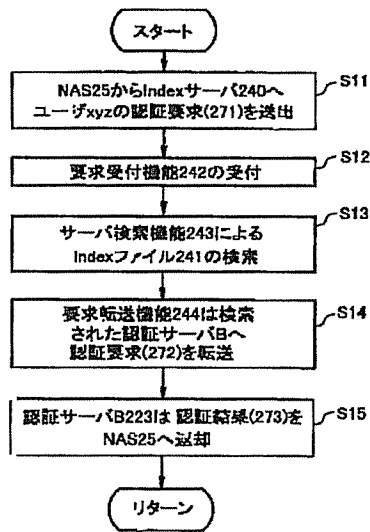
【図3】



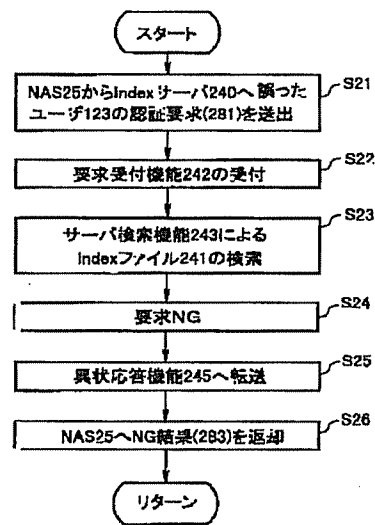
【図5】



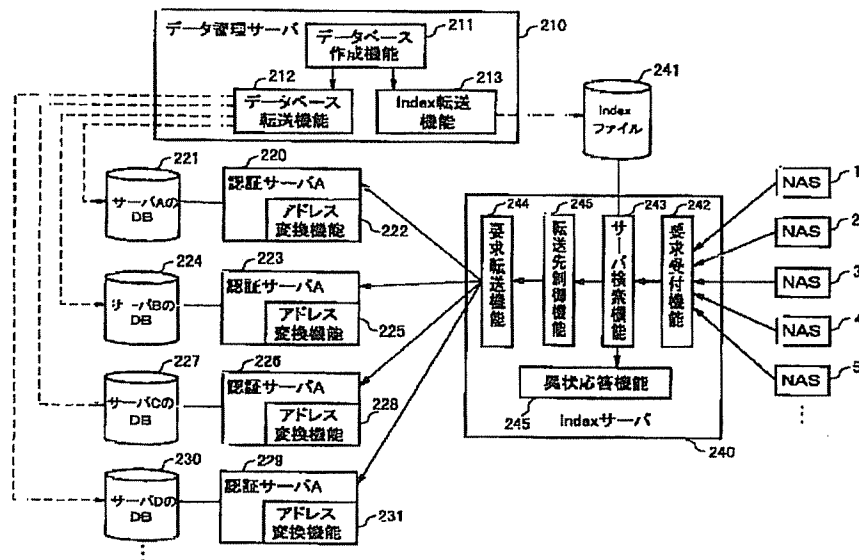
【図6】



【図7】



【図8】



【図10】

